DRUGS ON DEMAND

From the archive room to the hard drive

In the study "The World's Technological Capacity to Store, Communicate, and Computer Information", appearing on Feb. 10 in Science Express (digital journal that provides select Science articles ahead of print) calculates the world's total technological capacity: how much information humankind is able to store, communicate and compute.

From 1987 to 2007, Hilbert and López researched 60 categories of analog and digital technologies, and the results reflect our near complete transition from the analog to the digital age.

"In the year 2000, 75% of all information was still in analog format, mainly analog video cassettes (like VHS)," Hilbert says. And although analog technologies will always remain to exist, in 2002, just two years later, digital information became dominant, they estimated. "In 2007, 94% of our global technological memory consisted of digital bits and bytes." This is a big shift in the way we store data and how we can access this information.

The study states that as of 2007, humankind was able to store at least 295 exabytes (a number with 20 zeros) of information, communicate almost 2 quadrillion megabytes, and carry out 6.4 trillion MIPS (million instructions per second) on general-purpose computers.

A very poetic analogy Hilbert and López give is that all this digital information is enough to cover the entire area of the United States or China in 13 layers of books.

- -

In the case of surveillance

The panopticon surveillance prohibits the user to act natural, because he knows he's being watched, while the post-panopticon construction (there is no tower in the middle, no guards to be seen, Poster, 1990) relies on invisible surveillance. All the prisoners/users are being watched, they just do not see it.

I can compare this to illegal activities on college campus in relation to the material world and the digital one.

A couple of students found out what the concequences of surveillance through Facebook were: a university in Atlanta, USA, charged certain Facebook group members with 'conduct violations' after the members posted information regarding their alcohol use on-campus (Buckman, 2005) and four students at Northern Kentucky University (Buckman, 2005) were charged after posting photos of themselves consuming alcohol in a dorm room.
One could argue that it is just plain stupidity what these students did, and that it is just as much common knowledge that facebook is being monitored as that there are CCTV camera's and other security on campus. Still there is a difference: the physical presence of these surveillance instruments has an immediate and deep impact, that alters the way we handle situations. On Facebook there is not a two-way webcam stream with the board of directors staring into your dorm. You can't see who visited your profile. Even if you have all the privacy setting on 'alert alert danger danger', chances are your friends are going to upload pictures of you of that party you went to last week.

The same goes for drug dealing. What used to happen in specified (almost allocated) parts of the city, usually shady, deserted places like dark alleyways or subway stations, now is organized through online platforms such as fora and social networking websites, also reaching out to a much greater audience. This causes the police to not only monitor the 'shady places', because online, these illegal activities are not bound to place and time, everything has to be surveilled because everything is a potential risk. 'Harmless' platforms with a very different intention can be easily abused to follow the needs of the 'cybercriminal'. Or, another way of putting it: it all seems so harmless, innocent people can easily do unlawful acts, because the platform allows them. Now this raises a question: do these platforms need more restrictions? Would more surveillance help? Would 'cybercrime' just find another way (as it has done so far). What does more surveillance mean for privacy?

Also Danah Boyd has something to say about social networking sites.
"Social network sites are yet another form of public space. Yet, while mediated and unmediated publics play similar roles in people's lives, the mediated publics have four properties that are quite unique to them.
- Persistence. What you say sticks around. This is great for asynchronous communication, but it also means that what you said at 15 is still accessible when you are 30 and have purportedly outgrown those childish days.
- Searchability. My mother would've loved the ability to scream "Find!" into the ether and determine where I was hanging out with my friends. She couldn't, and I'm thankful. Today's teens' parents have found their hangouts with the flick of a few keystrokes.
- Replicability. Digital bits are copyable; this means that you can copy a conversation from one place and paste it into another place. It also means that it's difficult to determine if the content was doctored.
- Invisible audiences. While it is common to face strangers in public life, our eyes provide a good sense of who can overhear our expressions. In mediated publics, not only are lurkers invisible, but persistence, searchability, and replicability introduce audiences that were never present at the time when the expression was created.
These properties change all of the rules."

<<something about Net neutrality>>
DPI (Deep Packet Inspection).
"When you send an e-mail across the Internet, all your text is bundled into packets and sent on to its destination. A deep packet inspection device literally has the ability to look inside those packets and read your e-mail (or whatever the content might be). Net neutrality is based on the belief that nobody has the right to filter content on the Internet. Deep packet inspection is a method used for filtering. Thus, there is a conflict between the two approaches." What is DPI used for?
1) Targeted advertising
2) Reducing "unwanted" traffic (Bittorrent)
3) Block offensive material
4) Government spying (In the case of Iran (and to some extent China) and in Egypt as recent as February 2011) as to control and censor the internet.

Under the concept of 'lawful intercept', Nokia Siemens Networks sold products to Iran to monitor online traffic, with the purpose of intercepting data that relates to terrorism, child pornography, drug trafficking and other criminal activities carried out online.

But in as a reaction to all this surveillance, some kids are trying to joke around with their invisible audiences. At George Washington University, USA, college students played a prank on the watchful campus police. They advertised a massive beer blast on Facebook, but when campus police arrived to bust them, all they found was 40 students and a table with cake and cookies decorated with the word 'beer' (Hass 2006).

About the negative implications of Facebook ('Alcohol, Sex and Illegal Activities: An Analysis of Selected Facebook Central Photos in Fifty States' by Watson, Sandy White; Smith, Zachary; Driver, Jennifer):
"In addition, according to Heer and boyd (2005) some users have even used these sites to sell drugs"

Selling a piece of hash to your friends on Facebook is one thing, finding a dealing through fora is another. Mail Order Marijuana (MOM) is a concept that allows you to pay a certain person (preferably in cash via the mail), and then receive marijuana in a letter back. This can go back and forth for a long time, and these dealers have a lot of clients.
"Websites are hidden from search engines like Google. Most experts agree that the given the scale and anonymity of the internet, the online drug trade is unstoppable.
'It's not policeable. There are not enough cops in the world to monitor all the communications and digital commerce that's going on.'"
Every once in a while a distributor of marijuana does get caught, for sending marijuana to an undercover cop, or sometimes the mail gets intercepted at the post distribution centre. The recipients then try to find new dealers again on their fora.
Caution is key when involving oneself in such practices, before you know it you find yourself with an empty wallet and no marijuana in the mail. Because of course we do not hold any rights, nor can we apply the ten commandments of online shopping: such as checking the domainregister, paypal support, face to face transactions, etc. The same policies that restrict our privacy is not there to protect us.

On a more advanced base the mafia is also engaged in crimes such as drug trafficking, firearm dealing and prostitution. In the analog days the phone was used to make appointments, the police used to tap these landlines and sometimes the bad guys would get caught. While technology matures, it becomes harder for the criminal investigation department to maintain their grip on law enforcement.
Peer-to-peer based VoIP technologies such as Skype pose a technical challenge for surveillance because it's impossible to simply tap communications in a telephone exchange. In addition, Skype use a proprietary encryption method, which further complicates the matter.

Also drug cartels in Mexico make use of the internet to broaden their activities. They post videos on Youtube to intimidate enemies and recruit new members. One video opens with: "Esto es lo que le pasa a todos mis enemigos" ("This is what happens to all my enemies.") Happy Mexican music starts and a slideshow of annihilated police officers, crime scenes, dead bodies.
The U.S. Drug Enforcement Administration monitors the videos for clues about the cartels and potential use as evidence in prosecutions, says Garrison Courtney, a DEA spokesman. "It's really changed, how we target the cartels" he says.
The cartels "absolutely" post videos and have an online presence.
And online presence is persistent. Even if Youtube takes down a video, someone else has already downloaded it and uploads it again.

"21 April 2005
U.S. Authorities Break Online Drug-Trafficking Ring. Arrests of 20 people made in United States, four foreign countries. U.S. law enforcement agencies are announcing arrests in connection with an online drug-trafficking ring peddling pharmaceuticals such as steroids, narcotics and amphetamines, according to an April 20 press release from U.S. Immigration and Customs Enforcement (ICE)."

<<Prescription drug problem.>>

- -

<<ok what's next??>>
-link more to drugs, story of purple pokeballs on ebay and other 'candy'
-new drug in england, unlisted, so legal to ship anywhere
-prescription drugs story!
-in what other ways are online services being abused for illigal activities? how are institutions responding?
-prostitution via dating websites
-mafia organising crimes via skype (untracable)
-example of boy's baby sister on marktplaats
-me selling dogs on marktplaats
-flashing xbox marktplaats ad gets removed weekly
-paradox of infantilisation of crime vs higher surveillance/zero tolerance and punishment (=> at what cost? privacy is undermined, and still we are easily scammed!
-10 anti scam rules

<<central questions>>
-how do new media change the way crime is organized? (abuse of platforms, connectivity enlarges the audience)
-what consequences does this have for the way we are monitored/surveilled by government and websites (look into policies) (invisible surveillance)

- -

MENTAL NOTES
without media: if you haven't seen it it hasn't happened.
with media (cctv, online) everything is surveilled. is harder to do illegal stuff, creditcard instead of money is traced. but also has opened doors, can reach more people, also stuff is harder to trace like skype calls. no more illegal stuff in dark alleys.

how have illegal practices benefited and not benefited from new media?
organized crime vs. unorganized crime
exploitation of platforms.

in the name of surveillance and keeping order, the privacy of the citizens is being suppressed by the government. Government is sticking nose into our business, and they're excused because of terrorism reasons and whatnot. But going back to these criminal organisations and how they use the internet: how is all this extra surveillance changing the way they organize their crimes?

website policies/laws (Facebook > germany, google/gmail > china)
ebay is not a nation. choose another website or exploit the website? there's always people that exploit, should you change policy or not?
exploitation practices. survey more on that, more surveillance or take it as something that people really want to do so the policy should change?
laws should portray what people feel is wrong and right. but websites are not nations, it's privately held.
distinction between legal and illegal stuff, depend on country which you come from. either talk about stuff that is illegal (prostitution, drugs), or things that are in a grey zone (concerttickets, dogs, artwork).
should we either higher or lower the surveillance? back up with examples, for instance the boy who tried to sell his little sister, it was an innocent act.
how can you make a change in the system if you don't have a say in it. policies forbid you things so you are stuck sometimes if you want to do something (change privacy restrictions)
talk about Facebook as a nation (mark zuckerberg as a president). policy on nude pictures on Facebook. somebody is looking at your Facebook/ myspace pictures and judges if you are too nude. is this what we want?

fears of activities vs. realities of these activities (these books are more available)

Wendy Chun
Sadie Plant
Jussi Parikka Digital Contagions

<<This is a draft, messy, incomplete.>>